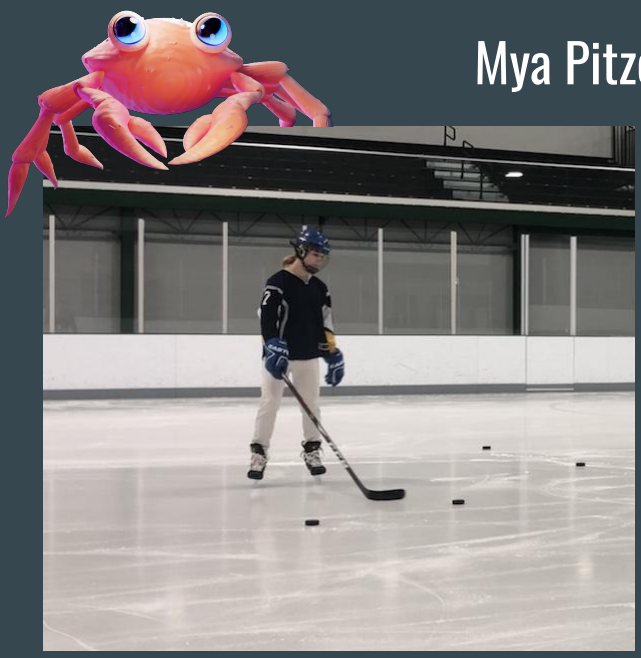
SecretOps for StartUps Using 1Password

•••

Legends Room
11:50 to 12:10



CrabNebula

- Company behind Tauri open source project
- Spent last year building a globally available distribution network for desktop applications
- “Third-party app store” kinda solution

Work history

Mom

- 1 kid, 3 dogs, 2 cats

Hockey player

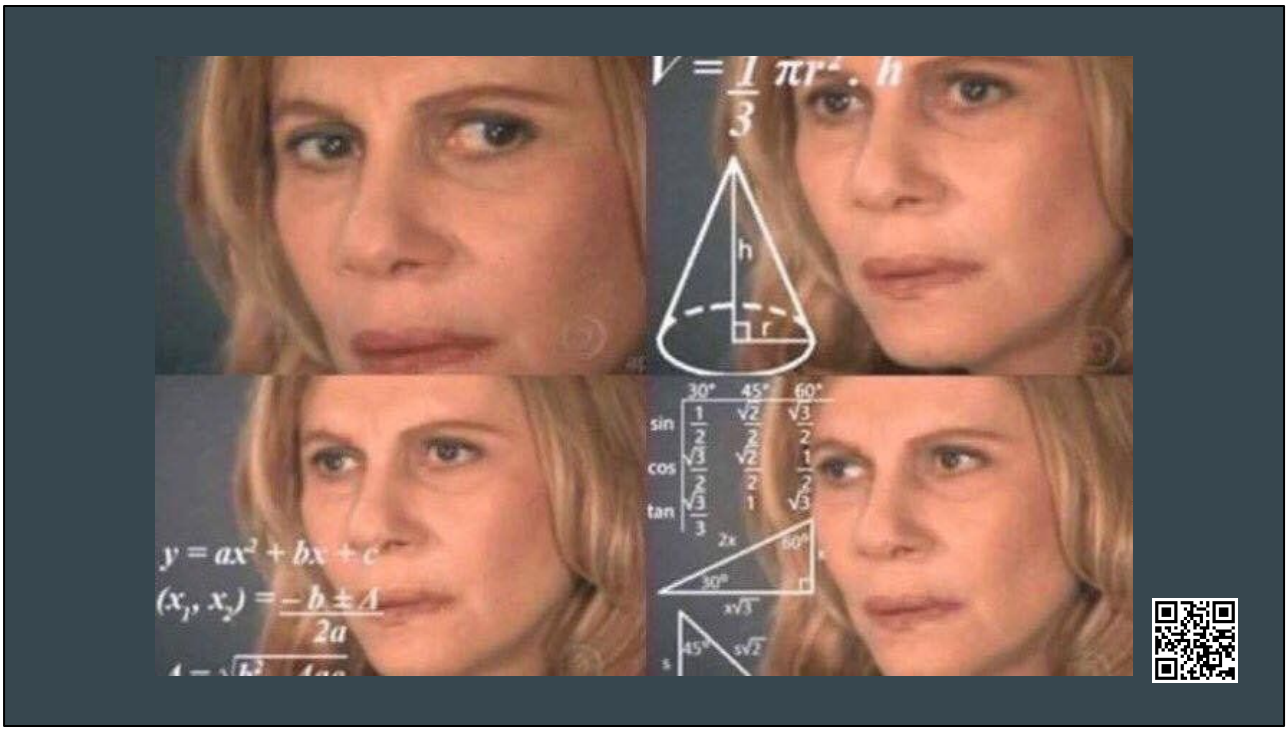
- 27 years
- Broke my first bone 5mo ago

Search and rescue

- Volunteer to search for missing persons… usually elderly folks with dementia or children at large events
- Can probably beat you in a game of hide-and-seek

QR code to LinkTree

- Links to social can be found at the bottom…
- Lots of other fun things on there too…



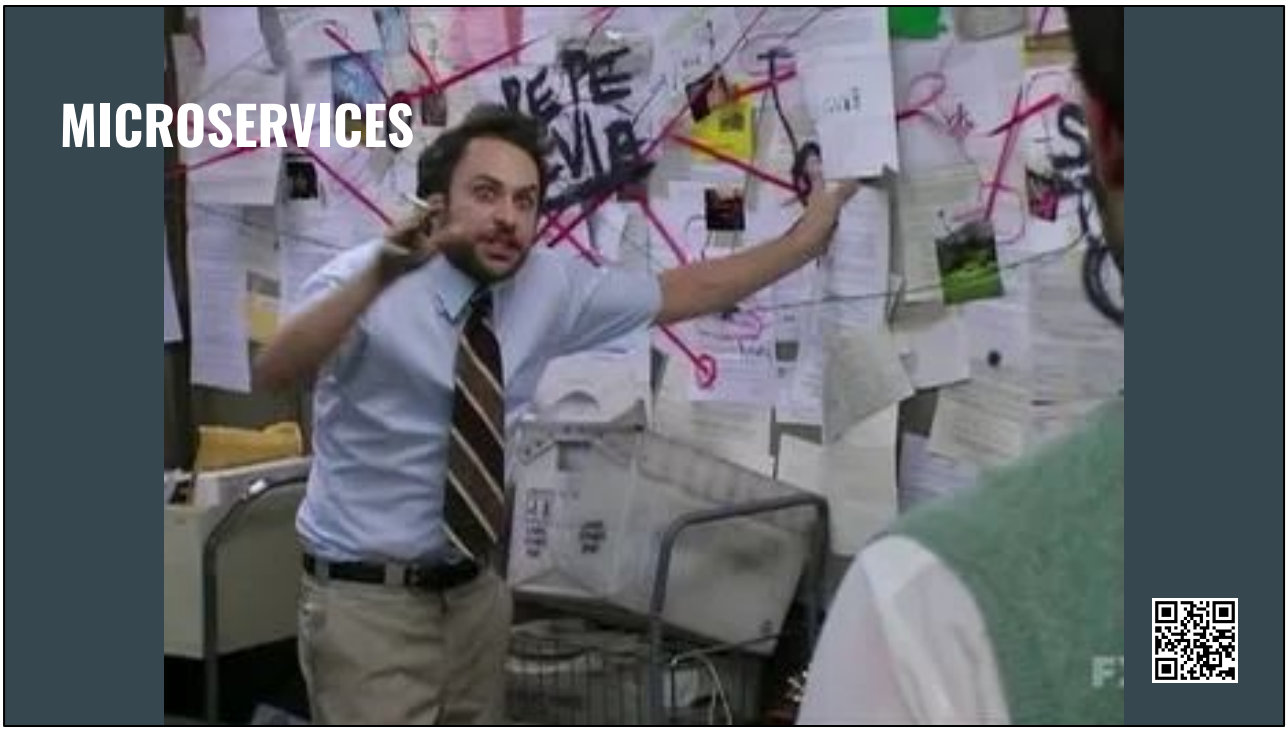
Often face some interesting challenges, especially in devops…

Work with a limited operations staff…

NEED to involve more members of the development team…

Often need to decide between doing something the “right” way, or doing something in a “reasonable” way. Trade offs:

- Cost
- Technical requirements
- Complexity



Systems today are becoming increasingly more complex.

Operations are expected to be experts on more systems, spreading them thin or requiring more support.

- You can see this both in private code bases, as well as public open-source projects as well.

Grafana + Prometheus now require Loki, Tempo, Mimir, or Thanos….
Securing runtime environments requires numerous systems from policy-enforcement agents, to low-level networking agents.

Many monolithic systems are splitting their runtime components into microservices to address scaling challenges, while also increasing the complexity of their system.

Software license changes often leave organizations scrambling to figure out whether their use of a system still falls within the scope of the new license.

Secret operations is one area we see a large number of solutions varying in complexity.

The problem is… StartUps and SMBs are often overlooked when setting pricing.

- Limited features for a price they can afford
- At the expense of doing things “right”

https://www.wsj.com/articles/indeeds-price-changes-leave-small-businesses-feeling-burned-43edf62

- SMBs were the initial target market

Increasing need to protect data

- User / Customer information
- Employee information
- Ownership
    - Walk away from a solution that you know is not working
    - With your data
    - Knowing it hasn't been compromised

Global Data Protection Regulations

US proposes 'know your customer' cloud computing requirements
- Reuters

Wants and Needs

- Accessible solution
- Doesn't break the bank
- Offers a reasonably secure solution
- Platform agnostic (sorry Kubernetes folks)

Accessible solution
- Used by both developers, operations, traditional IT

Doesn't break the bank

Offers a reasonably secure solution
- It doesn't need to be "perfect"
- Ideally should enable easy migration

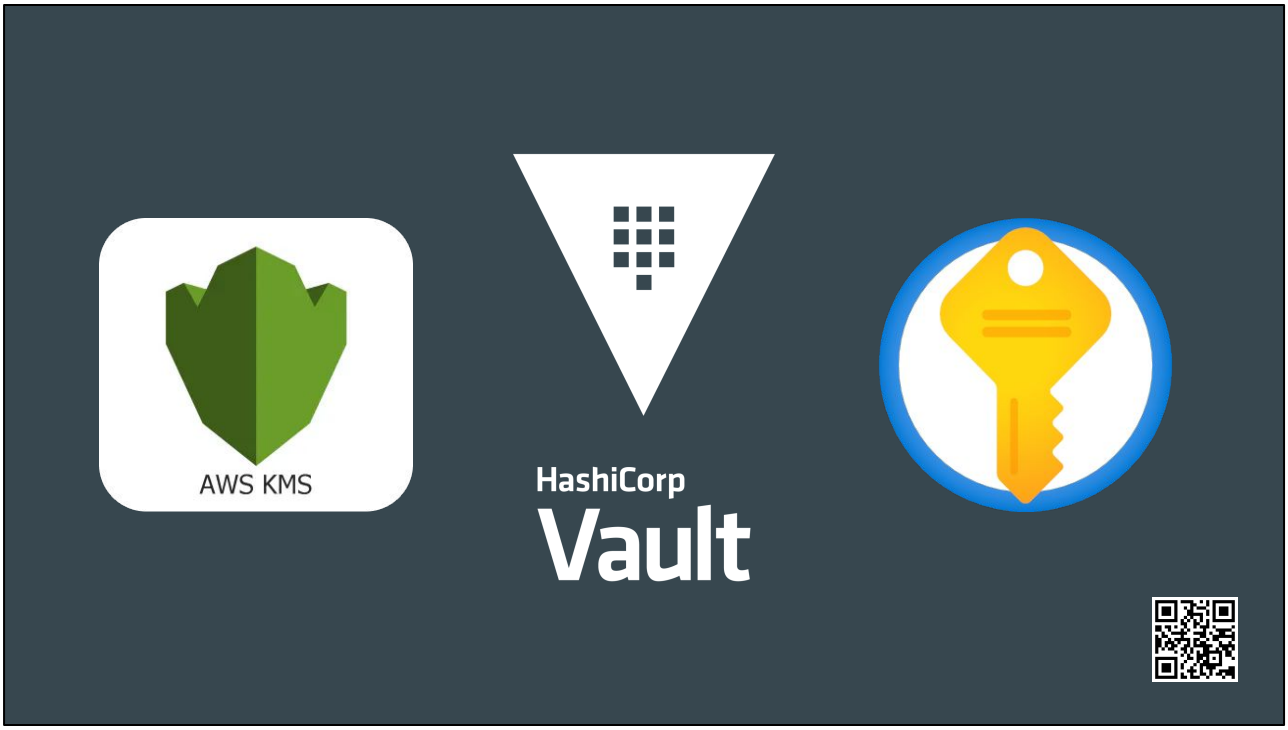
Platform agnostic (sorry Kubernetes folks)
- Should work with docker
- fly.io
- Heroku
- etc.…

SOPS

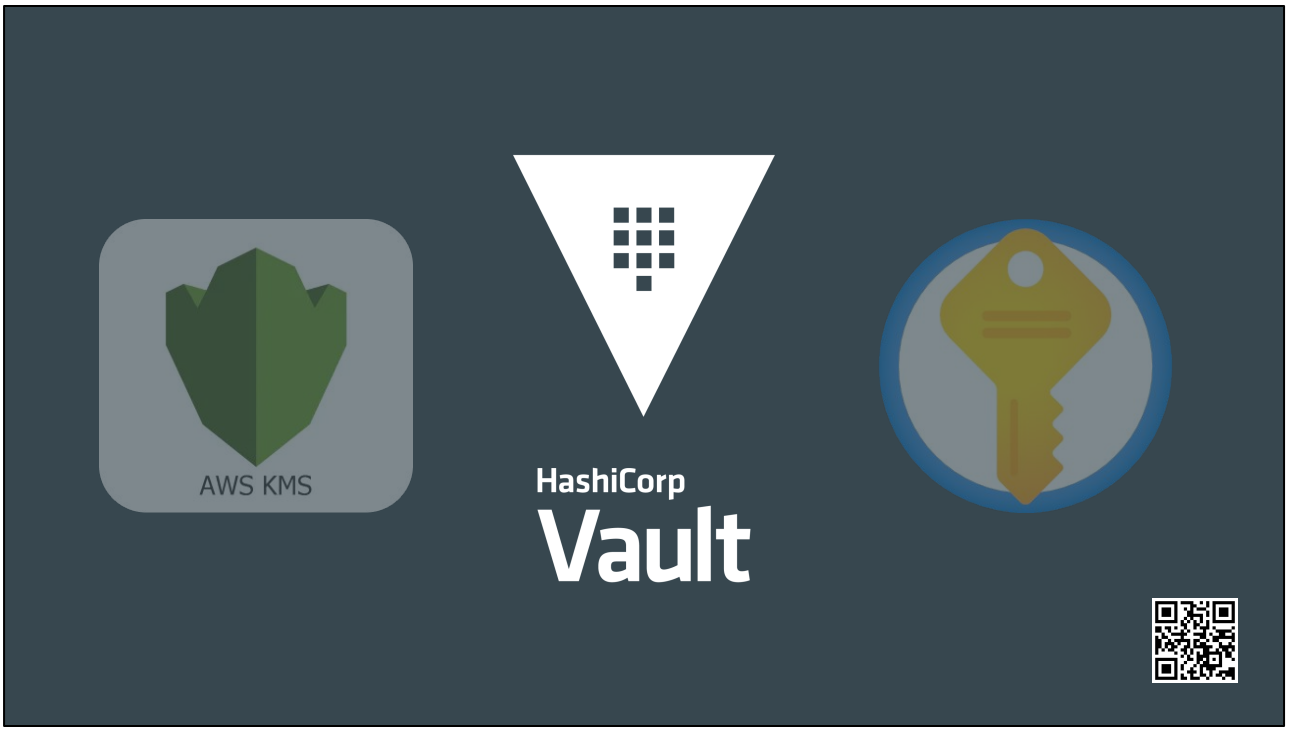
- Encrypt the values in common configuration files.
- Supports various KMS solutions out of box.
- Once a file is decrypted, the individual has access to all the secrets within that file.
- Some alternatives, but none are as feature rich.

SOPS

- YAML, JSON, env, properties, and more.
- No support for symmetric key encryption.
- GPG, AWS KMS, Google KMS, Azure Key Vault, Vault, and many more…
-
- https://github.com/getsops/sops
- https://opensource.com/article/19/2/secrets-management-tools-git



- KMS technologies are a dime a dozen
- Many clouds provide hosted solutions
- If you want to own your data, Vault is really the only option at the time of recording…



Popular option amongst larger organizations for handling centralized secret management.

- Secrets engine (dynamically generate credentials for databases)
- Auth methods (login with… assign identities)
- Audit sinks
- Policies
- Enforcement

Clustering

- Not easy to do
- Requires 3 or more instances
- Can be enabled with Consul
- Must be unsealed by an operator after each restart using k-of-m keys..
    - Shamir Secret Sharing

Possible Cons

- Relicensing concerns
- Recently acquired by IBM

Vault is a great piece of technology…. But it's complex, and often overkill for smaller environments.

If you’re going to run SOPS + Vault, you might just look at using Vault directly and dropping the SOPS support.

- In Kubernetes, Vault has an operator and secret injector process that can insert secret values directly into your pods that are created in the cluster.

1Password

Most organizations use some sort of password management solutions these days.

Popular choice among organizations.

Reasonably priced solution on the market.

Large number of developer focused features.

- SSH key management, GPG agent integrations, git commit signing, command line tool
- Can make repeatable setup of machines easy and intuitive

Other notable features…

- Generate secure password
- Template items for easy creation
- Item history (audit log)

Secret references

Usage

```
op://VAULT_NAME/ITEM_NAME/ATTRIBUTE_NAME
```

Basic

```
op://company_qa/example_database/password
```

Advanced

```
op://company_${TARGET_ENV}/example_database/password
```

There are a few different solutions that you can leverage.

Regardless, you'll need to be familiar with how these secret references look.

Command line - env files

```
op run --env-file 1password.env docker compose up -d
```

```
# 1password.env

DDA_POSTGRES_VERSION="latest"

DDA_POSTGRES_USER="op://DevOpsDays-demo-${TARGET_ENV}/postgres/user"

DDA_POSTGRES_PASSWORD="op://DevOpsDays-demo-${TARGET_ENV}/postgres/password"
```

Ideal for small to medium sized companies with a small number of operationally focused individuals.

https://github.com/mjpitz/mjpitz/blob/main/infra/helm/.env

Command line - configuration files

```
op inject -i base.json -o config.json
```

```
# base.json

{

  "dda_postgres_version" : "latest",

  "dda_postgres_user" : "{{ op://DevOpsDays-demo-${TARGET_ENV}/postgres/user }}"  ,

  "dda_postgres_password" : "{{ op://DevOpsDays-demo-${TARGET_ENV}/postgres/password
}}"

}
```

Ideal for small to medium sized companies with a small number of operationally focused individuals.

https://github.com/mjpitz/mjpitz/blob/main/infra/helm/.env

Kubernetes

- Operator => Push items into 1Password Vaults.
- Injector => Replaces secret references in Kubernetes resource with values.
- The HashiCorp Vault operator is similar, but different...

- Operator
  - https://developer.1password.com/docs/k8s/k8s-operator/
  - Shorthand for a service that responds to resources in Kubernetes
  - Operators can come in all shapes and sizes
- Injector
  - https://developer.1password.com/docs/k8s/k8s-injector
  - Webhook that mutates resources that are created / updated in the Kubernetes API
  - Looks at secrets, configmaps, and pods to replace secret references with their associated values
- HashiCorp Vault
  - Does have an operator/injector… works a little different
  - Uses annotations to inject secrets into the pods
  - IMO… the 1Password operator / injector is easier

Demo

Conclusion

- 1Password is accessible to non-operations focused staff.
- Likely a tool you're already paying for.
- 1Password may not be as fully featured as something like Vault.
- Works with environment variables and configuration files.

Thank you!